WHAT IS CLAIMED IS:

1. An optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a plurality of radially long parts of a reflection film are removed partially, so that auxiliary data are recorded by a second method of modulation, which differs from the first method, the optical disk being characterized by:

the auxiliary data including a first identification data recorded therein for identifying individual optical disks; and

the main data including an impermissible part recorded therein which can be used with the first identification data and/or a specified password.

2. The optical disk described in Claim 1, and further characterized in that it is a read only type optical disk.

3. The optical disk described in Claim 1 or 2, and further characterized by a specified password being obtained through a specified operation with the first identification data.

4. The optical disk described in Claim 1 or 2, wherein, in addition to the first identification data for identifying individual optical disks, a cipher key for a cipher and/or a decoding key for a cipher is recorded in the auxiliary data.

5. The optical disk described in Claim 1 or 2, and further characterized by the first method of modulation being a method of 8-16 modulation, and the second method of modulation being a method of phase encoding modulation.

6. A method of permitting the use of a program, the method being characterized in that it comprises the steps of:

reproducing an optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a plurality of radially long parts of a reflection film are removed partially, so that auxiliary data are recorded by a second method of modulation, which differs from the first method, the auxiliary data including a first identification data recorded therein for identifying individual optical disks and a cipher key for a cipher and/or a decoding key for a cipher, the main data including an impermissible part recorded therein which can be used with the first identification data and/or a specified password;

reproducing the first identification data from the auxiliary data; and

enabling the impermissible part to be used and outputting it with the first identification data and/or the specified password.

7. The method of permitting the use of a program described in Claim 6, and further characterized by the specified password being obtained through a specified operation with the first identification data.

8. A method of cryptocommunication characterized in that it comprises the steps of:

reproducing in a first computer an optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a plurality of radially long parts of a reflection film are removed partially, so that auxiliary data are recorded by a second method of modulation, which differs from the first method, the auxiliary data including a first identification data recorded therein for identifying individual optical disks and a first cipher key for a cipher and/or a decoding key for a cipher;

reading the first identification data and the first cipher key from the auxiliary data;

obtaining a first cipher which is a first data enciphered with the first cipher key and cipher algorithm; and

sending the first cipher from a communication means of the first computer through a network to a second computer.

9. The method of cryptocommunication described in Claim 8, and further characterized by the cipher algorithm being read from the main data.

10. A method of cryptocommunication characterized in that it comprises the steps of:

reproducing main data from a first recording area of an optical disk in a first computer;

reproducing auxiliary data from a second recording area, the auxiliary data including a first identification data for identifying individual optical

disks and a first cipher key for a cipher and/or a decoding key for a cipher;

enciphering a first data in the first computer with the first cipher key in the auxiliary data by cipher algorithm to make a first cipher;

connecting to the second computer of a particular connection address through a network to send the first cipher and the first identification data in the auxiliary data;

receiving the first identification data and the first cipher in the second computer;

selecting the first decoding key which is the decoding key for the cipher corresponding to the first identification data received from a first decoding key database, where a relationship between the first decoding key and the first identification data is stored; and

decoding the first cipher on the basis of the first decoding key to obtain the first data.

11. The method of cryptocommunication described in Claim 10, and characterized in that it comprises the further steps of:

generating with a first means for generating ciphers in the first computer a second cipher key and a second decoding key paired with each other;

obtaining a third cipher which is the second cipher key enciphered with the first cipher key in the first computer; and

sending the third cipher to the second computer.

12. The method of cryptocommunication described in Claim 11, and characterized in that it comprises the further steps of:

decoding the received third cipher with the first decoding key to obtain the plaintext of the second cipher key in the second computer;

obtaining a fourth cipher which is the second data enciphered with the second cipher key; and

sending the fourth cipher to the first computer.

13. The method of cryptocommunication described in Claim 8, and further characterized in that, at the step of reproducing two or more cipher keys and/or decoding keys for public key cipher from auxiliary data which include public key cipher, at least one of the cipher keys and the decoding keys is an elliptic function cipher.

14. The method of cryptocommunication described in Claim 8, and characterized in that it comprises the further step of using an optical disk with auxiliary data including a connection address data of the second computer, and reproducing the connection address from the auxiliary data.

15. An optical disk recorder for modulating a main data by a first method of modulation and recording the data by radiating a laser beam through an optical lens on to the recording layer of a first recording area of an optical disk, the recorder being characterized by:

reproducing, before recording, the auxiliary data in a second recording area, where a first identification data and a first cipher key for a cipher and/or a decoding key for a cipher are recorded by a second method of modulation;

making a main cipher which is the main data enciphered with the first identification data and/or the first cipher key and particular cipher algorithm; and

recording the main cipher in the recording layer of the first recording area by the first method of modulation.

16. The optical disk recorder described in Claim 15, and further characterized by:

receiving in a reception part the second cipher which is the first data enciphered with second cipher algorithm and a recording permission data permitting recording the first data in an optical disk;

obtaining a second decoded data through decoding the second cipher with a second decoding means;

making a main cipher through enciphering the second decoded data with first cipher algorithm different from the second cipher algorithm and an auxiliary data in a cipher computing means; and

recording the main cipher in the first recording area of the optical disk only if the recording permission data is present.

17. The optical disk recorder described in Claim 16, and characterized by:

mounting an IC card having a computing unit therein;

inputting into the IC card the first identification data for identifying the disk of the auxiliary data;

computing the first identification data with the computing unit;

inputting the result of the computation into the cipher computing means from the IC card;

obtaining a main cipher which is an enciphered second decoded signal; and

recording the main cipher in the optical disk.

18. An optical disk reproducer characterized by

reading with an optical head and a first means of demodulation an optical disk including a first recording area, where a main cipher is recorded by a first method of modulation, the main cipher being a first data enciphered with a first identification data by a cipher means;

reproducing with the optical head and a second means of demodulation an auxiliary data recorded in a second recording area of the optical disk by a second method of demodulation; and

obtaining the first data by decoding the main cipher by means of the decoding means with the first identification data in the auxiliary data or a first auxiliary identification data which is obtained from the first identification data through a predetermined computation.

19. The optical disk reproducer described in Claim 18, and further characterized by the method of modulation-demodulation of the first means of demodulation being a method of 8-16 modulation-demodulation, and the method of demodulation of the second means of demodulation being a method of phase encoding demodulation.

20. The optical disk reproducer described in Claim 18, and further characterized by the decoding means including a number "n" of decoding keys, and selecting one of the decoding keys on the basis of a decoding key

identification data reproduced from the main data in the optical disk.

21. The method of permitting the use of a program described in Claim 6, and characterized in that it comprises the further steps of:

connecting a first computer through a network to the second computer with a particular address;

sending to the second computer the first identification data for identifying the disk in the auxiliary data;

computing in the second computer the first identification data through a particular cipher operation, and sending the resultant (obtained) password to the first computer;

computing the password and the first identification data in the decoding operation part of the first computer, and sending the resultant second decoding code to a cipher decoder; and

enabling an impermissible part of the main data in the optical disk to be used with the second decoding code by means of the cipher decoder.

22. A method of inspecting the illegal installation of a program, the method being characterized in that it comprises the steps of:

reproducing with a first computer an optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a reflection film is removed partially, so that auxiliary data are overwritten by a second method of modulation, which differs from the first method, the auxiliary data including a first identification data recorded therein

for identifying individual optical disks, the main data including a first program, an installation program for installing the first program in the hard disk in the first computer, and a communication program recorded therein;

reproducing the first identification data from the auxiliary data;

installing the first program in the hard disk;

recording in the hard disk the first identification data or the first auxiliary identification data which is obtained from the first identification data through a predetermined computation; and

sending, when the installed first program starts or performs a particular operation, the first identification data or the first auxiliary identification data by means of the communication program to a second computer connected through a network to the first computer; or

checking through the network the second identification data which corresponds to the first identification data in the hard disk of the second computer or the second auxiliary identification data which is the second identification data computed through a particular operation; and

limiting the particular operation of the first program or adding a particular operation when the first and second identification data coincide or the first and second auxiliary identification data coincide.

23. An optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a reflection film is removed partially in the form of radially long bars from which the data cannot be

read with the naked eye, so that auxiliary data are overwritten by a second method of modulation, which differs from the first method, at a lower recording density than the main data, the optical disk being characterized in:

that a first identification data for identifying individual optical disks is recorded in the auxiliary data;

that a first data is recorded in the main data in the first recording area of the optical disk, and

that a data associated with the first identification data is printed as a merchandise bar code which can be read by a merchandise bar code reader.

24. The optical disk described in Claim 23, and further characterized by the merchandise bar code being printed on the side other than the reproduction side of the optical disk.

25. A method of permission to use the program of a first data in an optical disk, the method being characterized in that it comprises the steps of:

reading a first identification data or a first auxiliary identification data with a merchandise bar code reader in a first computer from an optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a reflection film is partially removed, so that auxiliary data are overwritten by a second method of modulation, which differs from the first method, the auxiliary data including the first identification data recorded therein for identifying individual optical disks, the main data in the first recording area of the optical disk including an

impermissible part the use of which is not permitted, the optical disk having a bar code printed thereon from which the merchandise bar code reader can read the first identification data or the first auxiliary identification data associated with the first identification data;

sending the first identification data or the first auxiliary identification data through a network to a second computer;

computing with the second computer through a cipher operation on the basis of the first identification data to make a permission data which permits the use of an impermissible part;

sending the permission data to the first computer; and

printing the permission data on paper with a printing means by the first computer.

26. An optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is the first predetermined area in the first recording area, where a plurality of radially long parts of a reflection film are removed partially, so that auxiliary data are overwritten over the pits in a low frequency band for frequency separation from the main data, the optical disk being characterized by:

the auxiliary data including a first identification data recorded therein for identifying individual optical disks; and

the main data including an impermissible part recorded therein which can be used with the first identification data and/or a specified password.

27. The optical disk described in Claim 26, and further characterized by being a read only type optical disk.

28. The optical disk described in Claim 26 or 27, and further characterized by the specified password being obtained through a specified operation with the first identification data.